5

PRZEMYSŁAW ROGUSKI

Verantwortlichkeit der Staaten für von ihrem Territorium ausgehende Cyberangriffe

Odpowiedzialność międzynarodowa państw za cyberataki podjęte z ich terytorium

Celem opracowania jest odpowiedź na pytanie, czy – a jeśli tak, to w jakim zakresie – państwa ponoszą odpowiedzialność międzynarodową za cyberataki przeprowadzone za pośrednictwem infrastruktury technicznej ulokowanej na ich terytorium.

Zarówno doktryna, jak i praktyka obecna w szeroko rozumianej społeczności międzynarodowej zakładają, iż cyberataki dające się przypisać państwu wywołują jego odpowiedzialność międzynarodową wedle „tradycyjnych" zasad. Dotychczas jednak niewystarczająco opracowano kwestię obowiązków państwa w sytuacji, gdy cyberataki są przeprowadzane z jego terytorium, aczkolwiek nie mogą mu być bezpośrednio przypisane. Wypracowanie stosownych standardów wydaje się o tyle pilne i konieczne, że większość cyberataków jest dokonywana przez podmioty pozapaństwowe, choć przy zastosowaniu infrastruktury technicznej ulokowanej na konkretnym terytorium.

Struktura tekstu jest trzyczęściowa. W pierwszej, wprowadzającej części prezentuje się stan faktyczny oraz pewne aspekty techniczne niezbędne do zrozumienia problemu. Druga część jest poświęcona omówieniu aktualnego stanu prawa międzynarodowego i doktryny w odniesieniu do odpowiedzialności międzynarodowej państw za cyberataki. W trzeciej, głównej części opracowania omawia się koncepcję *cyber due dilligence*, a więc obowiązku dochowania należytej staranności pod względem zapobiegania szkodom wypływającym z infrastruktury technicznej będącej pod jurysdykcją państwa. W szczególności analizuje się tu, czy standard należytej staranności obowiązuje również w cyberprzestrzeni, a jeśli tak, to jakie konkretnie obowiązki nakłada na państwa.

Główną tezą, a zarazem konkluzją opracowania jest to, iż na podstawie dotychczasowych norm prawa międzynarodowego, m.in. zasady dobrego sąsiedztwa, państwa mają obowiązek przeciwdziałania cyberatakom podejmowanym z ich terytorium. Przeciwdziałanie to przyjmuje formę implementacji takich rozwiązań technicznych i prawnych, które pozwolą na skuteczne zwalczanie lub sankcjonowanie cyberataków dokonywanych z ich terytorium. Przy braku odpowiednich działań państwa ponoszą natomiast odpowiedzialność międzynarodową.

Международная ответственность государств за кибер-атаки предпринятые с их территории

Цель настоящей главы заключается в ответе на вопрос, несут ли государства и если да, то в какой степени, международную ответственность за кибер-атаки осуществляемые с помощью технической инфраструктуры, расположенной на их территории.

Доктрина, также как и практика, широко понятого международного сообщества признают, что кибер-атаки, которые могут быть приписаны государству, приводят к его международной ответственности сообразно «традиционным» правилам. До настоящего времени вопрос обязательств государств в ситуации, когда кибер-атаки осуществляются с его территории, однако не могут быть ему приписаны, не был достаточно разработан. Потребность создания соответствующих стандартов является необходимостью так, как большинство кибер-атак осуществляется негосударственными субъектами, но с применением технической инфраструктуры, расположенной на определенной территории.

Структура данного исследования состоит из трех частей. В первой, вводной части представлена фактическая ситуация и некоторые технические аспекты, необходимые для понимания проблемы. Вторая часть посвящена обсуждению текущего состояния международного права и взглядов доктрины по отношению к международной ответственности государств за кибер-атаки. В третьей, основной части этого исследования, обсуждается теория *cyber due dilligence*, согласно которой страны обязаны сохранять особую осмотрительность для предотвращения ущерба, который может возникнуть посредством технической инфраструктуры, находящейся под их юрисдикцией. В третьей части рассматривается в частности, применим ли стандарт должной осмотрительности к киберпространству, и если да, то какие конкретные обязательства возложены на государство.

Главным тезисом и одновременно выводом исследования является то, что на основе существующих норм международного права, в том числе принципа добрососедства, страны взяли на себя обязательство противодействовать кибер-атакам осуществляемым с их территории. Противодействие это принимает форму внедрения таких технических и правовых решений, которые

позволят эффективно бороться и санкционировать кибер-атаки. Соответственно отсутствие необходимых действий влечет за собой международную ответственность данного государства.

Verantwortlichkeit der Staaten für von ihrem Territorium ausgehende Cyberangriffe

Ziel des Beitrags ist die Antwort auf die Frage, ob – und falls ja, in welchem Umfang – Staaten völkerrechtliche Verantwortlichkeit für Cyberangriffe tragen, die mittels auf ihrem Staatsgebiet gelegener technischer Infrastruktur unternommen werden.

Sowohl das Schrifttum als auch Praxis der weit verstandenen Völkergemeinschaft gehen davon aus, dass Staaten für ihnen zurechenbare Cyberangriffe völkerrechtliche Verantwortlichkeit nach den „klassischen" Regeln tragen. Bisher noch ungenügend erforscht bleibt jedoch die Frage nach der Staatenverantwortlichkeit für Cyberangriffe, die zwar von dem Staatsgebiet aus unternommen werden, jedoch nicht dem Staat zugerechnet werden können. Das Herausarbeiten konkreter Standards und Normen scheint umso dringlicher und notwendiger, als die meisten Cyberangriffe von nichtstaatlichen Akteuren, aber von einem konkreten Staatsgebiet aus, unternommen werden.

Der Beitrag besteht aus drei Teilen. Im ersten, einführenden Teil werden der Istzustand und einige technische Grundlagen besprochen, die für das Verständnis des rechtlichen Problems unabdingbar sind. Der zweite Teil befasst sich mit einer Darstellung des aktuellen Stands des Völkerrechts und des Schrifttums im Bereich der Staatenverantwortlichkeit für Cyberangriffe. Im dritten Teil des Beitrags wird das Konzept einer *cyber due dilligence*, also einer Sorgfaltspflicht hinsichtlich der Verhinderung von Schäden, die aus unter staatlicher Jurisdiktion stehender technischer Infrastruktur erwachsen, besprochen. Insbesondere wird analysiert, ob eine Sorgfaltspflicht auch im Cyberspace besteht und falls ja, welche konkreten Pflichten sie den Staaten auferlegt.

Die Hauptthese und zugleich Schlussfolgerung des Beitrags ist, dass auf Grundlage bisheriger völkerrechtlicher Normen, u.a. dem Prinzip der guten Nachbarschaft, die Staaten eine Pflicht haben, von ihrem Territorium aus unternommene Cyberattacken entgegenzuwirken. Ein solches Entgegenwirken kann in der Implementierung verschiedener technischer und rechtlicher Lösungen bestehen, welche eine wirksame Bekämpfung und Sanktionierung von Cyberangriffen ermöglichen. Unternimmt ein Staat nichts gegen Cyberangriffe, trägt er völkerrechtliche Verantwortlichkeit.

I. Einleitung

Seit Beginn des 21. Jahrhunderts bilden Computernetzwerke zunehmend das Rückgrat der digitalen Weltwirtschaft und moderner Informationsgesellschaften. Besondere Bedeutung kommt dabei dem Cyberspace[1] zu, welcher „*alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen*" umfasst[2]. Dieser weltweit über das Internet zugängliche Informationsraum stellt ein Feld der Betätigung sowohl staatlicher, als auch privater Akteure dar. Durch die Verlagerung wirtschaftlicher und privater Aktivitäten „ins Netz" werden diese allerdings zunehmend für Cyberangriffe, die von den weltweiten Computernetzwerken ausgehen, verwundbar[3]. Die Zahl der Cyberangriffe steigt in den letzten Jahren rasant an, wobei sowohl staatliche, als auch privat genutzte Computernetzwerke und Webseiten zum Ziel werden. Die bekanntesten computergestützten Angriffe der letzten Jahre stellen etwa die Cyberoperationen gegen Estland und Georgien, das Computervirus Stuxnet oder das Hacken der Webseite von *Sony Entertainment* dar[4]. Im Hinblick auf Cyberangriffe stellen sich für das Völkerrecht drei konkrete Fragen: *erstens,* inwieweit das Völkerrecht im Cyberspace Anwendung findet, *zweitens*, wie die Staatenverantwortlichkeit für Cyberangriffe geregelt ist und *drittens*, ob Staaten auch dann völkerrechtlich verantwortlich sind, wenn

---

[1] Zwar funktioniert im deutschen Sprachgebrauch auch der Begriff „Cyber-Raum", der etwa in offiziellen Stellungnahmen der deutschen Bundesregierung verwendet wird, siehe etwa zuletzt die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE vom 10.12.2015, BT-Drucks. 18/6989. Allerdings wird im deutschsprachigen Schrifttum viel häufiger der deckungsgleiche und aus dem Englischen stammende Begriff „Cyberspace" verwendet, dessen Gebrauch sich der Autor im folgenden Beitrag anschließt.

[2] Definition der Bundesregierung, Bundesministerium des Inneren, *Cyber-Sicherheitsstrategie für Deutschland*, S. 2, abrufbar unter: https://www.bka.de/nn_234152/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/cyberSicherheitsstrategieFuerDeutschland.html [zuletzt abgerufen am: 11.03.2016].

[3] Unter Cyberangriffen versteht man zielgerichtete Handlungen zur Abänderung, Störung oder Zerstörung von Computernetzwerken und/oder der auf ihnen laufenden Programme und gelagerten Daten; für eine ausführliche Diskussion des Begriffs vgl. T. Keber, P. Roguski, *Ius ad bellum electronicum?*, „Archiv des Völkerrechts" 2011, S. 399–434.

[4] Vgl. NATO CCD COE (E. Tikk u.a.), *International Cyber Incidents: Legal Considerations* 2010, S. 14–89, abrufbar unter: https://ccdcoe.org/publications/books/legalconsiderations.pdf [zuletzt abgerufen am: 11.03.2016]; M. Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, „Just Security", 17.12.2014, abrufbar unter: https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ [zuletzt abgerufen am: 11.03.2016].

computernetzwerkgestützte Angriffe von ihrem Territorium aus vollzogen werden, sie aber nicht direkt dem Staat zugeschrieben werden können. Auf diese Fragen soll nachfolgend kurz eingegangen werden.

II. Staatenverantwortlichkeit für Cyberangriffe – aktueller Diskussionsstand

Es besteht mittlerweile weitgehender Konsens darüber, dass völkerrechtliche Normen im Cyberspace anwendbar sind. Zwar gibt es bisher lediglich ein großes internationales Abkommen, welches speziell auf Rechtsfragen des Internets eingeht – das Europarat-Übereinkommen über Computerkriminalität vom 23. November 2001[5]. Allerdings sind sich sowohl die Staaten[6], als auch das Schrifttum[7] darüber einig, dass vertrags- und gewohnheitsrechtliche Normen im Internet ihre Geltung behalten, soweit sie ihrem Wesen nach auf den Cyberspace anwendbar sind.

Trotz alldem bleibt die völkerrechtliche Bewertung konkreter Cyberangriffe weiterhin problematisch. Unsicherheit besteht dabei hinsichtlich beider Elemente eines völkerrechtlichen Delikts, d.h. sowohl bei der Subsumtion einer Handlung unter eine konkrete Verbotsnorm, als auch – und vor allem – bei der Zurechnung der Handlung zu einem Staat[8]. Der aktuelle Diskussionsstand soll dabei nachfolgend kurz wiedergegeben werden.

Hinsichtlich der völkerrechtlichen Qualifikation eines Cyberangriffs besteht weitgehende Einigkeit darüber, dass ein Cyberangriff im Prinzip unter die Verbotsnormen der Charta der Vereinten Nationen [UN-Charta][9] fallen kann. Er kann sowohl Gewalt im Sinne des Art. 2 Abs. 4 UN-Charta als auch einen bewaffneten, das Rech zur Selbstverteidigung auslösenden Angriff im Sinne des

---

5 Abkommen des Europarates über Computerkriminalität vom 23. November 2011, Sammlung Europäischer Verträge Nr. 185

6 Vgl. etwa für Deutschland: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE vom 10.12.2015, BT-Drucks. 18/6989, S. 4; für die USA: White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Mai 2011), S. 9; vgl. auch Bericht der Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security vom 24. Juni 2013, U.N. Doc. A/68/98, Rn. 11.

7 Pionierarbeit im polnischen Schrifttum leistete insbesondere J. Kulesza, *Międzynarodowe Prawo Internetu*, Poznań: Ars boni et aequi, 2010, S. 23ff.

8 Vgl. Art. 2 der Artikel über die Verantwortlichkeit von Staaten für völkerrechtswidriges Handeln, U.N. Doc. A/56/83, 3 August 2001.

9 Charta der Vereinten Nationen vom 26. Juni 1945, deutsche Fassung: BGBl. 1973 II S. 431.

Art. 51 darstellen[10]. Umstritten bleibt jedoch, unter welchen Voraussetzungen dies geschehen kann, da sich Cyberangriffe in ihren Zielen, ihrer Schwere und den angewandten Methoden unterscheiden: so fallen unter den Begriff „Cyberangriff" sowohl *Distributed Denial of Service* (*DDoS*)-Attacken, die lediglich den Zugang zu bestimmten Webseiten durch Überlastung der Server blockieren, als auch *Malware*-Programme, die – wie bei Stuxnet – eine Systemfehlfunktion erzeugen und damit eine physische Zerstörung von Computern oder durch diese gesteuerten Systemen herbeiführen. Nach einer verbreiteten und von Staaten[11] und Lehre[12] geteilten Ansicht soll – in Anlehnung an den vom Internationalen Gerichtshof im *Nikaragua*-Fall entwickelten *scale-and-effects-test*[13] – ein bewaffneter Angriff bzw. eine Gewaltausübung dann vorliegen, wenn sie ihrer Skala bzw. Effekten nach mit einem konventionellen bewaffneten Angriff bzw. Gewaltausübung vergleichbar sind (sog. „Effekt-Äquivalenz")[14]. Dies erscheint insoweit unstrittig, als Gewalt bzw. bewaffneter Angriff nicht an bestimmte Waffensysteme gebunden sind und Computernetzwerkangriffe durchaus eine vergleichbare zerstörerische Wirkung entfalten können. Sollten infolge eines Cyberangriffs also Tod, Verletzung oder Zerstörung von Eigentum eingetreten sein, ist eine Effekt-Äquivalenz unproblematisch feststellbar.

Jedoch sind die Fälle, in denen Cyberangriffe unmittelbare physische Folgen im beschriebenen Ausmaß hervorrufen, äußerst selten[15]. Viel schwieriger ist die Bestimmung der Vergleichbarkeit bzw. Äquivalenz von konventionellen und cybergestützten Angriffen in Fällen, in denen die physischen Auswirkungen gering (z.B. Ausfall von Servern) oder nicht gegeben sind (z.B. reine Zerstörung von Daten, bei denen jedoch Schäden in Millionenhöhe entstehen können). Um die Vergleichbarkeit besser beurteilen zu können, wurden von M.N. Schmitt Kriterien wie die Schwere des Angriffs im Hinblick auf die körperliche Unversehrtheit der Person oder Zerstörung von Eigentum, Unmittelbarkeit,

---

[10] Vgl. statt vieler M. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, „The Yale Journal of International Law" 2011, S. 421ff. (435).

[11] Vgl. Stellung der USA: Report of the Secretary-General, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/66/152, S. 14ff.

[12] Vgl. statt vieler: M.N. Schmitt (Hrsg.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, 2013 [hiernach: Tallinn Manual], Rule 11, S. 45, mwN.

[13] IGH, Urteil vom 27. Juni 1986, *Certain Military Activities in Nicaragua* (Nicaragua v. United States), I.C.J. Reports 1986, S. 14, Rn. 195.

[14] T. Keber, P. Roguski, *Ius ad bellum…*, S. 408.

[15] Bisher wird dies nur im Falle des Computervirus Stuxnet, der zur Zerstörung von Urananreicherungszentrifugen im iranischen Forschungslabor Natanz führte, angenommen.

Direktheit, Nachweisbarkeit und Ausrichtung ausgearbeitet[16], die auch von den Verfassern des *Tallinn Manuals* übernommen wurden[17]. Allerdings treffen die Schmitt-Kriterien im Schrifttum nicht nur auf Zustimmung, sondern auch auf Kritik. So schließen manche Autoren bspw. die Effekt-Äquivalenz von Angriffen, die bloß zu Datenverlust oder Softwareschäden führen, aus[18].

Ein weiteres Problem besteht in der Zurechenbarkeit der Cyberangriffe zu einem Staat. Dabei liegen die Schwierigkeiten eher auf der Beweis-, denn auf der Rechtsebene[19]. Zum einen ist bereits die Identifizierung der Urheber von computernetzwerkgestützten Angriffen wegen der Eigenschaften der verwendeten Technik schwierig. Betrachtet man etwa die DDoS Angriffe auf Estland, so ist festzustellen, dass daran etwa 85000 Computer aus 178 Staaten beteiligt waren[20]. Zudem werden von Angreifern oft Anonymisierungstechniken, etwa das Netzwerk „Tor", *Virtual-Private-Network*-Verbindungen, Proxies usw. verwendet[21]. Zwar existieren für den betroffenen Staat technische Möglichkeiten, diese Anonymisierungstechniken zu umgehen, wie eine Studie des *Institute for Defense Analyses* nachweist[22]. Dies behaupten auch die Vereinigten Staaten, die etwa den Hacking-Angriff auf *Sony Entertainment* Nordkorea zugeschrieben haben und sich dabei auf Faktoren wie die IP-Adressen der für den Angriff benutzten Computer, die Ähnlichkeit mit anderer von Nordkorea benutzter Schadsoftware in Bezug auf Code, Verschlüsselungsalgorithmen, Datenlöschmethoden, sowie über Fernaufklärungsprogramme (Spionage) erlangte Erkenntnisse stützten[23]. Allerdings bleibt unklar, inwieweit jeder einzelne dieser Faktoren eine belastbare Beweismethode darstellen kann, da sie allenfalls – durchaus verfälschbare – Indizienbeweise darstellen. So haben etwa die Autoren des *Tallinn Manual* in Bezug auf IP-Adressen in Regel 8 festgestellt,

---

16 M.N. Schmitt, *Computer Network Attack and the Use of Force in International Law*, „Columbia Journal of Transnational Law" 1999, Vol. 37, S. 885–937 (914, 915).

17 Tallinn Manual, Rule 11, S. 49ff.

18 K. Ziolkowski, *Computer Network Operations and the Law of Armed Conflict*, „Military Law and the Law of War Review" 2010, S. 47–94 (69–75).

19 Vgl. IGH, Urteil vom 27. Juni 1986, *Certain Military Activities in Nicaragua* (Nicaragua v. United States), I.C.J. Reports 1986, S. 14, Rn. 57.

20 NATO CCD COE (E. Tikk u.a.), *International Cyber Incidents…*, *op. cit.*, S. 20, 23.

21 N. Tsagourias, *Cyber attacks, self-defence and the problem of attribution*, „Journal of Conflict and Security Law" 2012, S. 229–244 (234).

22 Institute for Defense Analyses (D. Wheeler, G. Larsen), *Techniques for Cyber Attack Attribution*, IDA Paper P-3792.

23 J. Goldsmith, *The Sony Hack: Attribution Problems, and the Connection to Domestic Surveillance*, Lawfare vom 19.12.2014, abrufbar unter: https://www.lawfareblog.com/sony-hack-attribution-problems-and-connection-domestic-surveillance [zuletzt abgerufen am: 11.03.2016].

dass allein aus der Tatsache, dass ein Cyberangriff über die Cyber-Infrastruktur eines Staates geleitet wurde, noch keine Beweiskraft für die Zurechnung des Angriffes zu dem Staat erwächst[24].

Die oben beschriebenen Situationen offenbaren die rechtlichen und faktischen, sich aus den technischen Gegebenheiten des Internet ergebenden Probleme der direkten Zurechnung eines Cyberangriffs zum Staat. Ist jedoch mit einer gewissen Wahrscheinlichkeit klar, dass der Cyberangriff dem Staat selbst entstammt oder unter Verwendung seiner Internetinfrastruktur durchgeführt wurde, stellt sich die Frage, ob der Staat weitergehende völkerrechtliche Pflichten zur Verhinderung des Cyberangriffes hatte.

III. Das Prinzip der *Cyber Due Dilligence*

Im Schrifttum wird über die Pflicht zur Verhinderung von Cyberangriffen vor dem Hintergrund der im Völkerrecht anerkannten, aus der Gebietshoheit und dem Prinzip guter Nachbarschaft stammenden Gewährleistungspflichten diskutiert; dabei wird oft der Begriff *Cyber Due Dilligence* verwendet[25]. Es ist seit langer Zeit anerkannt, dass aus der souveränen Staatengleichheit und der Gebietshoheit dem Territorialstaat die Pflicht erwächst, im Rahmen der gebotenen Sorgfalt (*due dilligence*) dafür Sorge zu tragen, sein Staatsgebiet nicht für schädliche Aktivitäten gegenüber anderen Staaten genutzt wird[26]. Dieses auf dem Prinzip *sic utere tuo ut alienum non laedas* basierte Gebot ist als gewohnheitsrechtlicher Rechtssatz anerkannt[27]. Obschon eine allgemeine Pflicht zur Anwendung gebotener Sorgfalt unbestritten ist, so ist der konkrete Umfang dieser Pflicht im Hinblick auf Handlungs- und Unterlassungspflichten streitig und in verschiedenen Rechtsgebieten unterschiedlich geregelt[28]. Am weitesten ausgeprägt ist dieser Rechtssatz im Umweltrecht, wo die *International*

---

[24] Tallinn Manual, Rule 8, S. 40.

[25] Vgl. statt vieler M. Schmitt, *In Defence of Due Dilligence in Cyberspace*, „The Yale Journal Forum" 2015, S. 68–81 mwN.

[26] A. von Arnauld, *Völkerrecht*, C.F. Müller 2012, Rn. 338.

[27] *Trail Smelter* arbitration, U.S. v. Canada, 3 R.I.A.A. 1905, S. 1965; IGH, Urteil vom 9.04.1949, *Corfu Channel Case* (U.K. v. Albania), I.C.J. Reports 1949, S. 4.

[28] Die *International Law Association* hat hierbei in einer Studie aufgrund der Fragmentierung des Völkerrechts erhebliche Divergenzen zwischen den einzelnen Rechtszweigen festgestellt. Siehe: ILA Study Group on Due Diligence in International Law (D. French, T. Stephens), *First Report of 7 March 2014*, abrufbar unter: http://www.ila-hq.org/download.cfm/docid/8AC4DFA1-4AB6-4687-A265FF9C0137A699 [zuletzt abgerufen am: 11.03.2016].

Law Commission[29] und die Staatengemeinschaft[30] detaillierte Regeln und *best practices* festgelegt haben.

Derartige klare Regeln haben sich in Bezug auf den *Cyberspace* bisher noch nicht formen können, werden aber zurzeit zwischenstaatlich und im Schrifttum ausgiebig diskutiert. Ausgangspunkt dieser Diskussion bilden zwei Überlegungen. Wie bereits oben dargelegt, ist sich die Staatengemeinschaft weitgehend darin einig, dass für den Cyberraum keine neuen völkerrechtlichen Regeln geschaffen werden müssen; vielmehr gelte das bestehende Völkerrecht im Internet, allerdings müsse es in Bezug auf die technischen Gegebenheiten adaptiert und ausgelegt werden. Als erste Vorüberlegung wird somit die staatliche Gebietshoheit auf den *Cyberspace* übertragen: der Staat, auf dessen Gebiet sich Cyber-Infrastruktur befindet, besitzt Kraft seiner Souveränität das Recht zur Kontrolle der Infrastruktur und über sie laufender Cyberaktivitäten[31]. Als zweite Vorüberlegung wird davon ausgegangen, dass sich aus dieser Hoheit über Cyber-Infrastruktur auch die Pflicht ergibt, diese Cyber-Infrastruktur nicht für schädliche Aktivitäten gegenüber anderen Staaten zu benutzen oder benutzen zu lassen[32].

Zur Begründung dieser Pflicht wird allgemein auf das Urteil des IGH im Korfukanal-Fall zurückgegriffen, wo der Gerichtshof feststellte: „[*it is*] *every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*"[33]. Dieser Satz findet seinen Niederschlag etwa in Regel 5 des *Tallinn Manuals*. Wie die Verfasser des *Tallinn Manuals* allerdings selbst zugeben, ist die Anwendung dieser Regel in Bezug auf das Internet kompliziert[34]. Zum einen ist umstritten, inwieweit Staaten zur Verhinderung von schädlichen Aktivitäten, die von ihrer Cyber-Infrastruktur ausgehen,

---

[29] ILC, Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities, Report of the International Law Commission 2001, U.N. Doc. A/56/10.

[30] Stockholm Declaration, *Report of the United Nations Conference on the Human Environment* (Stockholm, 5–16 Juni 1972), 11 ILM 1416; Rio Declaration', *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/5/Rev.1.

[31] Tallinn Manual, Rule 1, Rn. 1; W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, [in:] *2012 4th International Conference on Cyber Conflict*, Hrsg. C. Czosseck, R. Ottis, K. Ziolkowski, Tallinn: NATO CCD COE Publications, 2012, S. 11–12.

[32] K. Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, [in:] *Peacetime Regime for State Activities in Cyberspace*, Hrsg. K. Ziolkowski, Tallinn: NATO CCD COE Publication, 2013, S. 164ff.

[33] IGH, Urteil vom 4 April 1949, *Corfu Channel Case* (U.K. v. Albania), [1949] ICJ Rep 4, S. 22: „es ist die Pflicht eines jeden Staates, die Nutzung seines Territoriums für Handlungen, die die Rechte anderer Staaten verletzen, nicht bewusst zuzulassen" [eigene Übersetzung].

[34] Tallinn Manual, Rule 5, Rn. 5.

verpflichtet sind. Der IGH spricht die Pflicht nur bezüglich solcher Aktivitäten aus, von denen der Territorialstaat Kenntnis hat. Bei der Vielzahl der privaten Nutzer des Internet und wegen der offenen Architektur des weltweiten Netzes ist es jedoch schwierig festzulegen, wann ein Staat von einem bevorstehenden oder bereits stattfindenden Cyberangriff Kenntnis haben muss[35]. Sicherlich setzen hier menschenrechtliche Verpflichtungen und das *free-flow-of-information* – Prinzip der staatlichen Kontrolle von Internetaktivitäten Grenzen.

Ein weiterer Grund, wieso die Ausgestaltung eines Standards der gebotenen Sorgfalt auch auf Widerstand der Staaten stößt[36], ist die fehlende Einigkeit in Bezug auf die Pflichten von Transitstaaten, also jener Staaten, über deren Cyber-Infrastruktur ein Cyberangriff durchgeführt wird, dessen Ursprung allerdings woanders liegt. Aus der offenen Architektur des Internets und der technischen Gegebenheit, dass sich elektrische Signale zu ihrem Ziel den Weg des geringsten Widerstands suchen, ergibt sich, dass ein Cyberangriff über die Netzwerke einer Vielzahl von Staaten geführt werden kann, ohne dass diese Staaten Kenntnis davon haben müssen. Daher hat sich etwa eine UN-Expertengruppe lediglich auf die Empfehlung – nicht aber die Pflicht – zur Verhinderung von Cyberangriffen einigen können[37].

Problematisch bleibt auch die Frage, ob alle Cyberangriffe, oder nur Cyberangriffe von einer gewissen Intensität Sorgfaltspflichten hervorrufen und schließlich, welche Rechtsfolgen sich an die Pflicht zur Verhinderung knüpfen[38]. Wegen der dargestellten Kontroversen bedarf der Inhalt der *due dilligence*-Pflicht in der Tat weiterer Klärung. Allerdings besteht nach Ansicht des Verfassers bereits jetzt ein Minimalstandard im Rahmen der Pflicht zur Anwendung angemessener Sorgfalt: dieser bezieht sich auf die Pflicht zur Zusammenarbeit mit dem betroffenen Staat, sobald der Territorialstaat von dem Cyberangriff Kenntnis erlangt hat.[39] Eine solche Pflicht lässt sich aus dem Prinzip der guten Nachbarschaft herleiten, welches vorsieht, dass der Staat auf begründete Einwände anderer Staaten reagieren und diese in Betracht ziehen muss. In Anlehnung an die ILC Artikel zur Verhinderung grenzüberschreitender Schäden[40],

---

35 M. Schmitt, *In Defence of Due Dilligence in Cyberspace*, The Yale Journal Forum 2015, S. 70.

36 *Ibid.*, S. 71.

37 U.N. Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (24. Juni 2013).

38 M. Schmitt, *op. cit.*, S. 72ff.

39 Vgl. auch J. Kulesza, *State responsibility for cyber-attacks on international peace and security*, „Polish Yearbook of International Law" 2009/XXIX, S. 139-152, abrufbar unter: http://ssrn.com/abstract=1668020 [zuletzt abgerufen am: 11.03.2016], dort S. 11.

40 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries (2001) UN Doc A/56/10.

in denen die angemessene Sorgfalt (*due dilligence*) in der Pflicht zur Risikoeinschätzung (Art. 7), Benachrichtigung und Information (Art. 8) und Konsultation über Vorsorgemaßnahmen (Art. 9) konkretisiert wird, kann daher der minimale Inhalt der *cyber due diligence* Pflicht darin gesehen werden, erstens die eigene Cyber-Infrastruktur technisch und rechtlich so zu regulieren, dass Cyberangriffe erkannt und verfolgt werden können und zweitens, dass der Territorialstaat mit dem betroffenen Staat bei Vorliegen eines Cyberangriffs zum Zwecke dessen Beendigung und Feststellung der Identität der Urheber kooperiert[41]. Die Verweigerung der Zusammenarbeit oder die ausbleibende Reaktion auf einen bekannten Cyberangriff, obwohl technische Möglichkeiten zu seiner Beendigung bestünden, würde damit die Verletzung einer völkerrechtlichen Pflicht und somit ein völkerrechtliches Delikt begründen.

IV. Schlussbetrachtungen

Die dargestellten Überlegungen betreffen eine teilweise bestehende, in ihrer auf das Internet bezogenen Konkretisierung aber noch im Entstehen befindliche Rechtsnorm. In Anbetracht der Schwierigkeit einer direkten Zurechnung von Cyberangriffen kommt der Pflicht zur Verhinderung vom eigenen Territorium ausgehender Cyberangriffe im Sinne der Pflicht zur Anwendung angemessener Sorgfalt eine besondere Bedeutung zu. Bereits heute zeichnet sich ab, dass Staaten auf das Grundlegende Prinzip zurückgreifen und sich bei Nichtbefolgung dieser Pflicht Selbsthilfemaßnahmen gegenüber dem Staat, von dessen Territorium aus der Cyberangriff ausgeht, vorbehalten. Trotzdem ist eine schnelle Konkretisierung des Inhalts der *cyber due dilligence* Pflicht erstrebenswert, um Rechtssicherheit zu schaffen. Es bleibt abzuwarten, ob das für 2016 angekündigte Tallinn Manual 2.0 dieser Aufgabe nachkommen kann.

[41] Vgl. auch J. Kulesza, *op. cit.*, S. 11.